UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,004	01/28/2004	Yingqing Lawrence Cui	08226/0200356-US0	5027

38880 7590 05/06/2010

Yahoo! Inc.
c/o Frommer Lawrence & Haug LLP
745 Fifth Avenue
NEW YORK, NY 10151

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
05/06/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/767,004	CUI ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-32 and 34-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-32 and 34-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-7, 9-32, and 34-45 are pending.

With respect to claims 41-44, it is recommended that Applicant adds the phrase "non-transitory" prior to "computer readable storage medium" in order to clearly specify that the medium is non-transitory and, therefore, cannot be a signal, so as to avoid any future issues with 101 in this regard.

Response to Arguments

1. Applicant's arguments filed 1/28/2010 have been fully considered but they are not persuasive.

Applicant argues that the cited references do not teach "receiving a request from the mobile device, and further receiving a gateway group identifier for a carrier gateway that is associated with the mobile device request".

With respect to Aura, Applicant refers to columns 4 and 5, with no mention of the other cited portions of the reference (although column 5 was not cited for the gateway group identifier). Applicant provides various arguments with respect to Aura, arguing that items such as a credential key or credential in Aura are not gateway group identifiers. First, one must define what, precisely, a gateway group identifier is. In performing various searches in the art for "gateway group identifier", "gateway group ID", and the like, the Examiner has not found that this gateway group identifier is known in the art. Nor is it defined in the instant application, other than to reference a gateway group identifier and refer to "an identifier indicating a grouping of the gateway". As the gateway group identifier is

not defined in the application, one must determine what this identifier actually is. A gateway is defined in the application. As an example, page 7, lines 5-10 of the specification of the instant application states that "Carrier gateway 106 may include any computing device capable of connecting with mobile device 102 to enable communications with another computing device, such as server 108, another mobile device (not shown), and the like. Such devices include personal computers desktop computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, servers, and the like." As one can see, a "carrier gateway" is any device that allows a mobile device to connect to another device. Therefore, this carrier gateway could be a router, access point, BTS, switch, modem, or any other device that allows for connections through it from a mobile device.

Next to define group. As the instant application does not define what a group may be or how a carrier gateway may be in a gateway group, one must look to the broadest reasonable interpretation that one of ordinary skill in the art would take. In the art, when one references a group of something, the general definition is that the group comprises one or more item that are associated with each other. As an example, a group of devices connected to a LAN would be the set of devices connected to the LAN, where there is at least one device connected to the LAN to make up the group. Therefore, in order to have a gateway group, one must have at least one device that is associated with the group (which could just be the single device) based on whatever grouping strategy one may wish to use (e.g. cooperating devices, devices that share

mutual trust, devices that are all of the same type, etc.). An identifier is well-known in the art to be any piece of identifying data (e.g. number, character string, bit string, or any other data that relates to or identifies the entity in any fashion).

Putting all of the pieces together, the definition for a gateway group identifier becomes any piece of identifying data that in some manner identifies a group of one or more devices that are associated with each other, wherein the device allows communication from a mobile device to another device. While Applicant keeps arguing that Aura does not make "any mention of a gateway group identifier for a carrier gateway" and similar arguments, Applicant has never defined what the gateway group identifier actually is. In taking the above defined broadest reasonable interpretation of the gateway group identifier, one will see that Aura teaches many pieces of data that fall within the definition of a gateway group identifier.

Aura, column 4, lines 32-65 discusses the various forms and capabilities of base stations. It describes that base stations can be gateway servers, general purpose or specialized computers, media (e.g. wireless) access points, gateway routers, and "any other computer or service that makes the decision of allowing or denying access to the network." This section also describes how the base stations are used to directly and/or indirectly route communications between mobile nodes and the communications network. As one can see, the base stations of Aura are the same as the carrier gateways of the instant application, as was defined above. Column 9, line 43 to Column 10, line 27 describes how base stations are linked via a shared key K_{net} and how this key is used to encrypt

the credentials for a particular mobile device, such that the credentials can be decrypted by another base station sharing the same key (within the same shared key group). This K_{net} being shared between the base stations that cooperate with each other would have to have been distributed at some point prior to usage. Therefore, K_{net} will be received by each base station that uses it (other than the entity that generated it), or parameters that identify the grouping and/or group's key will be received by each base station that generate the key. Therefore, at some point in time, the base station will receive the key or receive a parameter for generating the key. Either way, this key or parameter for generating the key is associated with the group of base station which are to share the key and, therefore, is an identifier for the group, in that only the group members (as they have the identifier) can form and/or use the key/parameter/identifier. Furthermore, this portion describes trust parameters that are added to the credential by the base station, and that "The trust parameters specify any information about the mobile nodes that base station 1 wishes to pass on to base station 2 (or any other base station)." As these trust parameters are explicitly (or implicitly as at the bottom of this cited portion) defined in the credential by one base station in order to be taken into consideration by another base station, they clearly correlate to the group of base stations that includes those base stations. As one example, the date and time of the previous full authentication can be a trust parameter, designated by one base station for consideration by another. This date and time is used by the other base station (as defined in other portions of Aura) to determine whether (or how

much) to trust the mobile device. This date and time is clearly a bit string of some form that is "of" the base station that generated it, is related to the group of base stations, and used by the group of base stations in determining trust levels to be granted to a mobile device.

The final cited portion for the gateway group identifier in Aura is column 13, line 64 to column 15, line 6. Although a large citation, it is highly relevant to gateway group identifiers. In this section, one can see a random initialization vector being used in combination with K_{net} for encrypting a credential with a node identifier therein. This random initialization vector is a form of identifier that must be shared by the group of base stations intended to access the credential. Therefore, it can be seen as a gateway group identifier. The section then goes on to describe global identifiers being within the credential, and nonces being used in place of or in combination with the identifiers. Such nonces are described as being in correspondence with related identity or payment information. The nonces are in the credential and are added by the base station (which as described above, is the same as the carrier gateway of the instant application). The nonces are then used by other base stations within the group of cooperating base stations that receive the credential. Column 14, lines 63-67 of Aura recite that "Further parameter, such as a base station identifier, a MAC (Media Access Controller) address and a random number generated by the mobile node may be included as arguments to $f^{(1)}$ to strengthen it against forwarding and denial-of-service attacks." As one can see, a base station identifier can be used in the system, such base station identifier clearly

correlating to a gateway group identifier, where a group can be one or more nodes. The section finally discusses synchronized clocks and a secure mechanism for synchronizing clocks. Clearly, having synchronized clocks within the gateway group provides for a gateway group identifier (e.g. the synchronized clock value that is shared by and identifies that each base station is a part of the group). As one can see from the definition set forth above, and the discussion of Aura, gateway group identifiers are indeed, rather broad, and read on many of the pieces of data within Aura.

Applicant also argues that "Buhle appears to discuss such credentials within the context of an application server and/or data server, neither of which are carrier gateways as is further required by the pending claim 1. Nor does any mention about ServerN by Buhle even suggest such required carrier gateway, let alone a gateway group identifier for the carrier gateway." As carrier gateway and gateway group identifier have been defined above, they will not be defined again. However, taking the definition of carrier gateway from the instant application, the middle-tier servers (sometimes referred to in other manners, such as application servers, or Server#; middle-tier servers will be referred to hereafter to encompass all of the intermediate servers discussed in Buhle) are clearly within the realm of any computing device capable of connecting with a device to enable communications with another computing device. While Buhle may not explicitly refer to the clients as mobile devices, in the combination of Aura in view of Kou and Buhle, the clients of Buhle correlate to the mobile devices of Aura. As one can see in Buhle, the middle-tier servers enable communication between the

clients (mobile devices of the combination) and the data server. Therefore, taking Applicant's own definition of carrier gateway, the middle-tier servers of Buhle clearly correlate to the carrier gateway of the instant application. As to the gateway group identifier portion, such definition being described in-depth above, Buhle teaches passing identifiers for the middle-tier servers to other middle-tier servers and the data server. As an example of this, column 5, lines 39-41 of Buhle stats that "the necessary credential is passed to the application server after the application server connects to data server 206 using its own identity and verification." As one can see, the application server's identity is passed to the application server (the application server corresponding to the carrier gateway of the instant application, as described above). Clearly this identity is some form of identifier (e.g. one of the examples given in Buhle is use of a username and password for a middle-tier server to authenticate itself). It is also clearly associated with this application server. As a gateway group may comprise one or more gateways associated with each other in some manner, this identity of the application server is a gateway group identifier. This identity is used in trust determinations as described extensively in the final office action dated 5/7/2009 and, therefore, will not be described in much detail here. However, suffice it to say that the identity and authorization of the/each middle-tier server is used in determining what the client's authorization will be at the data server.

Buhle also describes connecting through multiple middle-tier servers (Server1 through ServerN). This establishes a chain of trust in which each middle-tier server trusts the previous server to pass the appropriate data (this is

based on authentication of each middle-tier server by the next, where ServerN will trust the entire chain of middle-tier servers prior to it based on authentication of ServerN-1, going all the way down to Server2 trusting Server1 and Server3 authenticating Server2 and therefore, gaining the trust that Server2 has in Server1). This chain of trust forms of group of middle-tier servers (which, as described above, correlate to the carrier gateways of the present invention). As the client's data has passed through each middle-tier server to reach ServerN, and ServerN has authenticated itself to the data server, this clearly shows a gateway group identifier (e.g. the identity of ServerN, which is associated with the group of Server1 through ServerN as the chain of trust is formed by going through each of those servers) of the carrier gateway (e.g. ServerN) being received by the data server. A further gateway group identifier may be the chain of client identifiers that are provided through the middle-tier servers. As discussed in column 7, lines 45-59, each middle-tier server may use multiple identities for the client (e.g. an internal and external identity), wherein the middle-tier server passes both identities to the next middle-tier server. This continues down the line until the ServerN which will have the entire collection of client identities, this collection being specific to the group of middle-tier servers through which the communication passed. As one can see, using the broadest reasonable definitions of carrier gateway and gateway group identifier as one of ordinary skill in the art would see them based on the instant application's disclosure, the combination of Aura in view of Kou and Buhle clearly teaches "receiving a request from the mobile device, and further receiving a gateway

group identifier for a carrier gateway that is associated with the mobile device request".

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 18-25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 18 is directed to "A mobile device to communicate with a server over a network, the mobile device performs actions, comprising:". However, the claim still does not describe any actual hardware components of this mobile device. In order to be statutory as an apparatus, the claim must describe at least one hardware component of the mobile device, however, claim 18 merely describes actions that are performed by the mobile device. Examples of hardware are hard drives, microprocessors, or the like. An example of how to fix the claim may be to add a microprocessor that executes the actions, and a storage device that stores the actions within the body of the claim. Claims 19-25 only describe more actions, and do not include any hardware/physical components. Therefore, claims 19-25 are rejected for the same reasons. It is noted that in the previous response, the Examiner suggested both providing the claim to be directed to a mobile device as well as "providing the appropriate elements for tying in the code described in the claim with the device. As an

example, adding a processor that executes the code, and a storage medium that stores the code appears as though it would suffice." As only the former has been done, and it still requires hardware within the device itself.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 4, 9-12, 14, 15, 26-30, 32, 35-38, and 40-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura (U.S. Patent 6,947,725) in view of Kou (U.S. Patent 7,216,236) and Buhle (U.S. Patent 6,286,104).

Regarding Claim 1,

Aura discloses a method of managing a communication with a mobile device over a network, comprising:

Receiving a request from the mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23) and further receiving a gateway group identifier for a carrier gateway that is associated with the mobile device request (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

Automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23), and based on:

Using the associated information, determining if a trusted mobile device identifier associated with the mobile device is received (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

If the trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

If the mobile device is enabled to access the Internet, then determining at least a third level of trust associated with the mobile device (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19);

Determining at least one device signature for the mobile device based on the at least one level of trust from the plurality of different levels of trust, and independent of user authentication, the at least one device signature being useable to enable the mobile device to perform an action over the network associated with the request (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27);

But does not explicitly disclose determining if the mobile device is enabled to accept a cookie; determining if the mobile device is enabled to interact with a URL; and determining if the carrier gateway is trustable above a defined level using the gateway group identifier.

Kou, however, discloses using associated information of a request, determining a capability of the mobile device, including determining if the mobile device is enabled to accept a cookie, and determining if the mobile device is enabled to interact with a URL (Column 9, lines 23-42; and Column 15, lines 40-54);

If the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device (Column 9, lines 23-42; server requiring cookies to be enabled, and informing the client to enable cookies; if cookies remain disabled, the client is not allowed access); and

If the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device (Column 9, lines 23-42; and Column 15, lines 40-54; the client sending a request including a URL and/or the client using a specific URL format (e.g. HTTP or HTTPS) when HTTPS is required and the server ensuring that HTTPS is used). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure session

management techniques of Kou into the mobile authentication system of Aura in order to allow the system to enforce certain security restrictions, such as forcing clients to use a secure protocol, such as HTTPS, in order to access certain information, thereby ensuring security of the information that is to be protected.

Buhle, however, discloses receiving a gateway group identifier for a gateway that is associated with the mobile device request; using the gateway group identifier, determining if the carrier gateway is trustable above a defined level; and determining levels of trust based on both a device ID and whether the gateway is trustable above the defined level (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication and authorization system of Buhle into the mobile authentication system of Aura as modified by Kou in order to provide a highly dynamic system of roles and permissions such that a device connecting directly to a data server will have one set of roles/permissions and when the device connects through certain middle-tier servers, the roles and permissions change based on each server through which the connection is made, thereby providing a high degree of security, auditing, and dynamic system behavior based upon how the user connects to the system.

Regarding Claim 3,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses that the associated information comprises at least one of a device identifier, user agent information, and an indication that the mobile device is enabled to accept a cookie (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 4,

Aura as modified by Kou and Buhle discloses the method of claim 3, in addition, Aura discloses that the associated information further comprises at least one of a gateway group identifier and a subscription identifier (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 9,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses that the mobile device identifier is at least one of a MIN, ESN, application serial number, or a mobile telephone number (Column 13, line 64 to Column 15, line 6).

Regarding Claim 10,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises if the first level of trust is

determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 11,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises if the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 12,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises if the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 14,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises employing a hash function selected from at least one of a message digest, SHA, DES, 3DES, HAVAL, RIPEMD, and Tiger hash function (Column 4, lines 58-62).

Regarding Claim 15,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses expiring the at least one device signature based, in part, on a predetermined period of time associated with each of the at least one device signature (Column 9, line 43 to Column 10, line 27).

Regarding Claim 26,

Aura discloses a server for managing a communication with a mobile device over a network comprising:

A transceiver for receiving a request from the mobile device and for sending at least one device signature to the mobile device (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

A transcoder that is configured to perform actions including:

Receiving the request from the mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

Receiving a gateway group identifier for a carrier gateway (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

Automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23) and further based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

If the mobile device is enabled to access the Internet, then determining at least a third level of trust associated with the mobile device (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19); and

Determining the at least one device signature for the mobile device based on the at least one level of trust of the plurality of different trust levels, wherein the at least one device signature is independent of user authentication (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27);

But does not explicitly disclose determining if the mobile device is enabled to accept a cookie; determining if the mobile device is enabled to interact with a URL; receiving the gateway

group identifier from the carrier gateway, and determining if the carrier gateway is trustable.

Kou, however, discloses determining if the mobile device is enabled to accept a cookie, and if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device (Column 9, lines 23-42); and

Determining if the mobile device is enabled to interact with a URL, and if the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device (Column 9, lines 23-42; and Column 15, lines 40-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure session management techniques of Kou into the mobile authentication system of Aura in order to allow the system to enforce certain security restrictions, such as forcing clients to use a secure protocol, such as HTTPS, in order to access certain information, thereby ensuring security of the information that is to be protected.

Buhle, however, discloses receiving, from a gateway associated with a request from a mobile device, a gateway group identifier for the gateway and determining levels of trust based on both a device ID and whether the gateway is determined to be trustable (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52). It would have been obvious to

one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication and authorization system of Buhle into the mobile authentication system of Aura as modified by Kou in order to provide a highly dynamic system of roles and permissions such that a device connecting directly to a data server will have one set of roles/permissions and when the device connects through certain middle-tier servers, the roles and permissions change based on each server through which the connection is made, thereby providing a high degree of security, auditing, and dynamic system behavior based upon how the user connects to the system.

Regarding Claim 27,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses that the transcoder is configured to perform actions comprising receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and determining the at least one level of trust based, in part, on the associated information and the gateway information (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 28,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses that determining the at least

one device signature comprises if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 29,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses that determining the at least one device signature further comprises if the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 30,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses that determining the at least one device signature further comprises if the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random

number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 32,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses that determining the at least one level of trust further comprises determining the second level of trust based at least one of the gateway identifier, and a user agent (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 35,

Aura discloses a system for managing a communication with a mobile device over a network comprising:

The mobile device configured to provide information associated with the mobile device (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

A server, coupled to a carrier gateway, that is configured to receive the associated information and to perform actions (Column 4, lines 32-65; Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23), including:

Automatically determining at least two different levels of trust from a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and

Column 7, line 42 to Column 8, line 23), wherein the at least two different levels of trust are based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and

Determining another level of trust associated with the mobile device (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

Initially determining at least two different device signatures for the mobile device each of the two device signatures being based on a different one of the at least two different levels of trust, wherein the at least two device signatures are each determined independent of user authentication (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

But does not appear to explicitly disclose determining if the mobile device is enabled with a defined operational capability, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a URL, and determining if a gateway group identifier associated with a carrier gateway is trustable.

Kou, however, discloses determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a URL (Column 9, lines 23-42; and Column 15, lines 40-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure session management techniques of Kou into the mobile authentication system of Aura in order to allow the system to enforce certain security restrictions, such as forcing clients to use a secure protocol, such as HTTPS, in order to access certain information, thereby ensuring security of the information that is to be protected.

Buhle, however, discloses determining levels of trust based on both a device ID and whether a gateway group identifier associated with a carrier gateway is determined to be trustable (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication and authorization system of Buhle into the mobile authentication system of Aura as modified by Kou in

order to provide a highly dynamic system of roles and permissions such that a device connecting directly to a data server will have one set of roles/permissions and when the device connects through certain middle-tier servers, the roles and permissions change based on each server through which the connection is made, thereby providing a high degree of security, auditing, and dynamic system behavior based upon how the user connects to the system.

Regarding Claim 36,

Aura as modified by Kou and Buhle discloses the system of claim 35, in addition, Aura discloses that determining the at least two device signatures further comprises determining a tier 1 device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 37,

Aura as modified by Kou and Buhle discloses the system of claim 35, in addition, Aura discloses that determining the at least two device signatures further comprises determining a tier 2 device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 38,

Aura as modified by Kou and Buhle discloses the system of claim 35, in addition, Aura discloses that determining the at least two device signatures further comprises determining a tier 3 device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 40,

Aura as modified by Kou and Buhle discloses the system of claim 35, in addition, Aura discloses the carrier gateway, coupled to the mobile device, that is configured to receive the associated information, and provide the associated information and gateway information related to the carrier gateway (Column 4, lines 32-65; and Column 13, line 64 to Column 15, line 6); and Buhle discloses that the gateway is coupled to the mobile device and is configured to receive associated information and provide the associated information and gateway information, including the gateway group identifier, related to the gateway (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52).

Regarding Claim 41,

Aura discloses a computer readable storage medium for communicating with a mobile device, the computer readable

storage medium having computer executable instructions stored thereon that when installed into a computing device enable the computing device to perform actions, comprising:

Receiving a request from the mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23) and further receiving a gateway group identifier for a carrier gateway that is associated with the mobile device request (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

Sending at least one device signature to the mobile device based on at least one level of trust determined from a plurality of different levels of trust that is determined, in part, using the associated information (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27), wherein the at least one level of trust is based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and

Determining another level of trust associated with the mobile device, and wherein the at least one device signature is determined

independent of user authentication (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

But does not appear to explicitly disclose determining if the mobile device is enabled with a defined operational capability and determining if the gateway is trustable based on the gateway group identifier above a threshold.

Kou, however, discloses determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a URL (Column 9, lines 23-42; and Column 15, lines 40-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure session management techniques of Kou into the mobile authentication system of Aura in order to allow the system to enforce certain security restrictions, such as forcing clients to use a secure protocol, such as HTTPS, in order to access certain information, thereby ensuring security of the information that is to be protected.

Buhle, however, discloses receiving a gateway group identifier for a gateway that is associated with the mobile device

request; using the gateway group identifier to determine if the gateway is trustable above a threshold; and determining levels of trust based on both a device ID and whether the gateway is trustable above a defined level (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication and authorization system of Buhle into the mobile authentication system of Aura as modified by Kou in order to provide a highly dynamic system of roles and permissions such that a device connecting directly to a data server will have one set of roles/permissions and when the device connects through certain middle-tier servers, the roles and permissions change based on each server through which the connection is made, thereby providing a high degree of security, auditing, and dynamic system behavior based upon how the user connects to the system.

Regarding Claim 42,

Aura as modified by Kou and Buhle discloses the computer readable storage medium of claim 41, in addition, Aura discloses that determining the at least one device signature further comprises if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, a user agent identifier, and a

time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 43,

Aura as modified by Kou and Buhle discloses the computer readable storage medium of claim 41, in addition, Aura discloses that determining the at least one device signature further comprises if the other level of trust is determined, determining another device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 44,

Aura as modified by Kou and Buhle discloses the computer readable storage medium of claim 41, in addition, Aura discloses that determining the at least one device signature further comprises if the other level of trust is determined, determining another device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6)

Regarding Claim 45,

Aura discloses an apparatus for communicating with a mobile device comprising:

A means for receiving a request from a mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

Means for receiving a gateway group identifier associated with a carrier gateway for the request from the mobile device (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

A means for automatically determining a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

A means for determining a plurality of different device signatures for the mobile deice based, in part, on the determined plurality of different levels of trust, and independent of user authentication (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27);

But does not appear to explicitly disclose that the associated information indicates a capability of the mobile device, that at least one of the different levels of trust is based on an operational capability of the mobile device, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the

mobile device is enabled to interact with a URL, and determining if the gateway is trustable above a threshold.

Kou, however, discloses that the associated information indicates a capability of the mobile device and that at least one of the different levels of trust is based on an operational capability of the mobile device, wherein the other level of trust is determined based on at least one of a determination that the mobile device is enabled to accept a cookie and a determination that the mobile device is enabled to interact with a URL (Column 9, lines 23-42; and Column 15, lines 40-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure session management techniques of Kou into the mobile authentication system of Aura in order to allow the system to enforce certain security restrictions, such as forcing clients to use a secure protocol, such as HTTPS, in order to access certain information, thereby ensuring security of the information that is to be protected.

Buhle, however, discloses means for receiving a gateway group identifier associated with a carrier gateway for the request from the mobile device; using the gateway group identifier to determine if the gateway is trustable above a threshold; and determining levels of trust based on both a device ID and whether the gateway is trustable above a threshold based on the gateway

group identifier (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication and authorization system of Buhle into the mobile authentication system of Aura as modified by Kou in order to provide a highly dynamic system of roles and permissions such that a device connecting directly to a data server will have one set of roles/permissions and when the device connects through certain middle-tier servers, the roles and permissions change based on each server through which the connection is made, thereby providing a high degree of security, auditing, and dynamic system behavior based upon how the user connects to the system.

4. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Kou and Buhle, further in view of Bryson (U.S. Patent Application Publication 2004/0185777).

Aura as modified by Kou and Buhle does not explicitly disclose that the gateway group identifier is obtained from a header of a network packet associated with the carrier gateway.

Bryson, however, discloses that the gateway group identifier is obtained from a header of a network packet associated with the carrier gateway (Paragraph 91). It would have been obvious to one of ordinary

skill in the art at the time of applicant's invention to incorporate the portable wireless gateway system of Bryson into the mobile authentication system of Aura as modified by Kou and Buhle in order to allow devices of a wide variety of communication protocols to connect to and use the system, while allowing for moving access points such that users can spontaneously provision connectivity in many locations such as planes, trains, ships, and buses without having to preplan for their connectivity needs.

5. Claims 5, 18, 20-22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Kou and Buhle, further in view of Wilf (U.S. Patent 6,496,824).

Regarding Claim 5,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses automatically determining a second device signature based on a second level of trust, wherein the second device signature comprises a hash of at least a gateway group identifier (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); but does not explicitly disclose that the signature hash also comprises a cookie and a user agent identifier obtainable from the associated information.

Wilf, however, discloses that the signature hash also comprises at least a cookie and a user agent identifier obtainable

from the associated information (Column 4, lines 5-35). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management techniques of Wilf into the mobile authentication system of Aura as modified by Kou and Buhle in order to provide a stronger signature, based upon more client and/or gateway specific information, thus increasing security of the signature and making it harder to forge.

Regarding Claim 18,

Aura discloses a mobile device to communicate with a server over a network, the mobile device performs actions comprising:

Sending a request to the server for content, wherein the request includes an identifier associated with the device (Column 5, line 58 to Column 6, line 13; Column 7, line 42 to Column 8, line 23; and Column 13, line 64 to Column 15, line 6); and wherein the server also receives a gateway group identifier associated with a carrier gateway (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

Receiving at least one device signature associated with the mobile device, wherein the at least one device signature is based on at least one level of trust determined from a plurality of different trust levels, and is independent of user authentication (Column 5,

line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23), the at least one level of trust being determined based on:

Determining at least a default level of trust (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19);

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and

If the mobile device is enabled to access the Internet, then determining at least a third level of trust associated with the mobile device (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19); and

But does not appear to explicitly disclose determining if the mobile device is enabled to accept a cookie, determining if the mobile device is enabled to interact with a URL; that the identifier associated with the device comprises an identifier associated with a user agent, and determining if the gateway is trustable based on the gateway group identifier.

Kou, however, discloses determining if the mobile device is enabled to accept a cookie, and if the mobile device is enabled to

accept a cookie, then determining at least a second level of trust associated with the mobile device (Column 9, lines 23-42); and

Determining if the mobile device is enabled to interact with a URL, and if the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device (Column 9, lines 23-42; and Column 15, lines 40-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure session management techniques of Kou into the mobile authentication system of Aura in order to allow the system to enforce certain security restrictions, such as forcing clients to use a secure protocol, such as HTTPS, in order to access certain information, thereby ensuring security of the information that is to be protected.

Buhle, however, discloses that a gateway associated with the request further provides a gateway group identifier; determining if the gateway is trustable based on the gateway group identifier;; and determining levels of trust based on both a device ID and whether the gateway is trustable (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication and authorization system of Buhle into the mobile authentication system of Aura as modified by Kou in order to provide a highly dynamic

system of roles and permissions such that a device connecting directly to a data server will have one set of roles/permissions and when the device connects through certain middle-tier servers, the roles and permissions change based on each server through which the connection is made, thereby providing a high degree of security, auditing, and dynamic system behavior based upon how the user connects to the system.

Wilf, however, discloses that the identifier associated with the device comprises an identifier associated with a user agent (Column 4, lines 5-35). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management techniques of Wilf into the mobile authentication system of Aura as modified by Kou and Buhle in order to provide a stronger signature, based upon more client and/or gateway specific information, thus increasing security of the signature and making it harder to forge.

Regarding Claim 20,

Aura as modified by Kou, Buhle, and Wilf discloses the mobile device of claim 18, in addition, Aura discloses that receiving the at least one device signature further comprises if the at least one device signature is based on the first level of trust, receiving a first tier device signature based, in part, on a hash of at least one of a subscription identifier, the gateway group identifier, the user

agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 21,

Aura as modified by Kou, Buhle, and Wilf discloses the mobile device of claim 18, in addition, Aura discloses that receiving the at least one device signature further comprises if the at least one device signature is based on the second level of trust, receiving a second tier device signature based, in part, on a hash of at least one of a cookie, the gateway group identifier, the user gent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 22,

Aura as modified by Kou, Buhle, and Wilf discloses the mobile device of claim 18, in addition, Aura discloses that receiving the at least one device signature further comprises if the at least one device signature is based on the third level of trust, receiving a third tier device signature based, in part, on a hash of at least one of the gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 24,

Aura as modified by Kou, Buhle, and Wilf discloses the mobile device of claim 18, in addition, Kou discloses that receiving the at least one device signature further comprises, if the request indicates the mobile device is enabled to accept a cookie, associating the cookie with the at least one device signature (Column 8, lines 26-53; and Column 9, lines 6-42); and Wilf discloses associating the cookie with the at least one device signature (Column 4, lines 5-35).

6. Claims 6, 7, 16, 17, 31, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Kou and Buhle, further in view of Laraki (U.S. Patent Application Publication 2003/0233329).

Regarding Claim 6,

Aura as modified by Kou and Buhle does not explicitly disclose that the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a MIN, ESN, and application serial number.

Laraki, however, discloses that the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a MIN, ESN, and application serial number (Paragraph 53). It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou and Buhle in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 7,

Aura as modified by Kou and Buhle discloses the method of claim 1, in addition, Aura discloses determining the level of trust of the mobile device identifier and trusting the mobile device if the identifier is so trusted (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and Buhle discloses determining a level of trust of the carrier gateway associated with the mobile device based on a received device identifier and the gateway group identifier (Column 5, line 25 to Column 6, line 25; Column 6, lines 61-67; and Column 8, lines 20-52);

But does not appear to explicitly disclose using a received subscription identifier in the determining of a level of trust, trusting the mobile device identifier based on such carrier trust, and inhibiting the determination of a level of trust associated with the device if the mobile device identifier is not trusted in this manner.

Laraki, however, discloses determining a level of trust of a carrier associated with the mobile device based on at least one of a received subscription identifier and a gateway group identifier, trusting the mobile device identifier based on such carrier trust, and inhibiting the determination of a level of trust associated with the device if the mobile device identifier is not trusted in this manner (Paragraphs 33-37 and 46-72). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou and Buhle in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 16,

Aura as modified by Kou and Buhle does not explicitly disclose if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

Laraki, however, discloses if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature (Paragraphs 45 and 66). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou and Buhle in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 17,

Aura as modified by Kou, Buhle, and Laraki discloses the method of claim 16, in addition, Laraki discloses that determining if the expired device signature is to be rolled over further comprises evaluating at least one of a condition, event, change in an identifier indicating a grouping of the gateway, and a time (Paragraphs 45 and 66).

Regarding Claim 31,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses that determining the at least one level of trust further comprises determining the first level of trust based at least one of a gateway group identifier, a subscription identifier, a user agent, and a security level associated with the request from the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

But does not appear to explicitly disclose using such information to determine if the mobile device identifier is trusted.

Laraki, however, discloses using such information to determine if the mobile device identifier is trusted (Paragraphs 33-37 and 46-72). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou and Buhle in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 34,

Aura as modified by Kou and Buhle discloses the server of claim 26, in addition, Aura discloses determining if at least one device signature has expired (Column 13, line 64 to Column 15, line 6); but does not explicitly disclose extending a validity period associated with the expired device signature is the expired device signature is to be rolled over.

Laraki, however, discloses determining if at least one device signature has expired and extending a validity period associated with the expired device signature is the expired device signature is to be rolled over (Paragraphs 45 and 66). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou and Buhle in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

7. Claims 13 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Kou and Buhle, further in view of Kindberg (U.S. Patent Application Publication 2003/0061515).

Regarding Claim 13,

Aura as modified by Kou and Buhle does not explicitly disclose including a device signature in a munged URL.

Kindberg, however, discloses including a device signature in a munged URL (Paragraphs 39 and 43-50). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability-enabled URL of Kindberg into the mobile authentication system of Aura as modified by Kou and Buhle in order to provide a simple mechanism by which a client can prove authorized access to resources via use of a modified URL including a signature corresponding to a particular capability.

Regarding Claim 39,

Aura as modified by Kou and Buhle does not explicitly disclose providing a signature to the mobile device through a munged URL.

Kindberg, however, discloses providing a signature to the mobile device through a munged URL (Paragraphs 39 and 43-50). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability-enabled URL of Kindberg into the mobile authentication system of Aura as modified by Kou and Buhle in order to provide a simple mechanism by which a client can prove authorized access to resources via use

of a modified URL including a signature corresponding to a particular capability.

8. Claims 19 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Kou, Buhle, and Wilf, further in view of Laraki.

Regarding Claim 19,

Aura as modified by Kou, Buhle, and Wilf does not explicitly disclose providing the mobile device identifier based on at least one of a MIN, an ESN, and an application serial number.

Laraki, however, discloses providing the mobile device identifier based on at least one of a MIN, an ESN, and an application serial number (Paragraph 53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou, Buhle, and Wilf in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 23,

Aura as modified by Kou, Buhle, and Wilf discloses the mobile device of claim 18, in addition, Aura discloses data in the form of at least one device signature (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); but does not appear to explicitly disclose that sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions comprising: modifying the request to include at least one of a subscription identifier associated with the mobile device and a gateway identifier; forwarding the modified request to the server; receiving data from the server; and forwarding the data to the mobile device.

Laraki, however, discloses that sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions comprising: modifying the request to include at least one of a subscription identifier associated with the mobile device and a gateway identifier; forwarding the modified request to the server; receiving data from the server; and forwarding the data to the mobile device (Paragraphs 33-37 and 46-48). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Kou, Buhle, and Wilf in order to efficiently provide mobile users with access to

content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

9. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Kou, Buhle, and Wilf, further in view of Kindberg.

Aura as modified by Kou, Buhle, and Wilf does not explicitly disclose receiving a munged URL associated with at least one device signature.

Kindberg, however, discloses receiving a munged URL associated with at least one device signature (Paragraphs 39 and 43-50). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability-enabled URL of Kindberg into the mobile authentication system of Aura as modified by Kou, Buhle, and Wilf in order to provide a simple mechanism by which a client can prove authorized access to resources via use of a modified URL including a signature corresponding to a particular capability.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437